1 Naši noví kamarádi: Eukleidés, Bézout a Euler

Zadání
Verze ze dne 21. února 2024

Cíle cvičení: Důkladně si procvičíme Eukleidův algoritmus nad celými čísly, zejména si uvědomíme, že s jeho pomocí umíme počítat inverzní prvky v konečným tělesech a také některé kongruence. Na závěr se naučíme vzoreček pro výpočet Eulerovy funkce.

Úlohy, které bychom určitě měli umět řešit:

Nejprve připomeňme rozšířený Eukleidův algoritmus hledání největšího společného dělitele přirozených čísel a_0 a a_1: Položíme $(u_0, v_0) := (1, 0)$, $(u_1, v_1) := (0, 1)$ a $i = 1$ a pak dokud $a_i > 0$ počítáme $a_{i+1} := (a_{i-1}) \bmod a_i$, $q_i := (a_{i-1}) \operatorname{div} a_i$ a dále hodnoty $(u_{i+1}, v_{i+1}) := (u_{i-1},\ v_{i-1}) - q_i(u_i, v_i)$ a $i = i + 1$. Výstupem je potom $a_{i-1} = \mathrm{NSD}(a_0, a_1)$ a Bézoutovy koeficienty u_{i-1}, v_{i-1} splňující $\mathrm{NSD}(a_0, a_1) = u_{i-1}a_0 + v_{i-1}a_1$.

Úloha 1.1. Najděte $\mathrm{NSD}(37, 10)$ a příslušné Bézoutovy koeficienty. Spočítejte 10^{-1} v tělese $\mathbb{Z}_{37}$.

Úloha 1.2. Najděte $\mathrm{NSD}(1023, 96)$ a příslušné Bézoutovy koeficienty.

Úloha 1.3. Najděte nějaké celočíselné řešení rovnice $1023x + 96y = 18$.

Úloha 1.4. Najděte 27^{-1} v tělese $\mathbb{Z}_{41}$.

Připomeňme si, že je-li $n \in \mathbb{N}$, pak pro celá čísla a, b definujeme $a \equiv b \pmod n$ právě tehdy, když $n \mid (a - b)$. Z přednášky dobře víme, že pro $a \equiv b \pmod m$ a $c \equiv d \pmod m$ platí $a \Box c \equiv b \Box d \pmod m$, kde $\Box$ je některá z operací $+, -, \cdot$ a dokonce $a \equiv b \pmod m \Leftrightarrow ac \equiv bc \pmod{mc}$, což je ekvivalentní $ac \equiv bc \pmod m$ za předpokladu, že c a m jsou nesoudělná.

Úloha 1.5. Vyřešte v celých číslech následující kongruence:

(a) $x \equiv 2 \pmod 8$,

(b) $3x \equiv 2 \pmod 5$,

(c) $27x \equiv 16 \pmod{41}$,

(d) $6x \equiv 2 \pmod 8$ (pozor na změnu modulu, když „dělíme dvojkou“),

Úloha 1.6. Ukažte, že $n^2 \equiv 1 \pmod 8$ pro každé liché $n \in \mathbb{N}$.

Úloha 1.7. Určete hodnotu Eulerovy funkce

(a) $\varphi(600)$,

(b) $\varphi(7425)$ (mohlo by se hodit vědět, že $7425 = 27 \cdot 25 \cdot 11$).

A teď něco pro zábavu a rozšíření obzorů:

Úloha 1.8. Najděte NSD$(89, 55)$ a příslušné Bézoutovy koeficienty. Jak se na výpočtu a výsledku projeví, že jedná o dva po sobě jdoucí členy Fibonacciho posloupnosti?

Úloha 1.9. Spočtěte NSD$(2^{92} - 1, 2^{31} - 1)$ a příslušné Bézoutovy koeficienty.

Úloha 1.10. Spočtěte NSD$(2k+1, 3k+1)$ a příslušné Bézoutovy koeficienty v závislosti na $k \in \mathbb{N}$.

Úloha 1.11. Je možné uvažovat inverzní prvek a^{-1} také modulo m, které není prvočíslo? Co třeba 29^{-1} nebo 33^{-1} v okruhu $\mathbb{Z}_{39}$? Jak to souvisí s (ne)soudělností?

Úloha 1.12. Vyřešte v celých číslech následující kongruence:

(a) $x^2 + 5x \equiv 0 \pmod{19}$,

(b) $x^2 \equiv 1 \pmod{p}$ pro p prvočíslo,

(c)* $x^2 + 10x + 6 \equiv 0 \pmod{17}$.

Úloha 1.13. Najděte všechna čísla n taková, že $\varphi(n) = 18$.

Úloha 1.14. Najděte všechna čísla $n > 1$ taková, že $\varphi(n) \mid n$

Úloha 1.15. Označme $\sigma(n)$ součet všech dělitelů přirozeného čísla n. Najděte vzorec pro výpočet $\sigma(n)$, pokud znáte prvočíselný rozklad čísla n. Inspirujte se důkazem vzorce pro Eulerovu funkci

Úloha 1.16.* Najděte všechna $x, y, z, w \in \mathbb{Z}$ splňující $x^2 + y^2 + z^2 = 15w^2$ (*Návod:* řešte nejprve kongruenci modulo 8.)

Úloha 1.17.* Pomocí modulární aritmetiky odvoďte kritéria dělitelnosti pro čísla 9 a 11.

Úloha 1.18.* Ukažte, že století (pokud se nezmění kalendář) nikdy nebudou začínat středou, pátkem ani nedělí. (1. ledna 2001 bylo pondělí.)